Information Security Policy

Visar Systems AB | Version 1.0 | 25 November 2026

Policy owner: Simon Ekman, CEO

Approver: Board of Directors

Board approval date: 2026-11-26

Purpose and scope

Visar Systems AB will protect the confidentiality, integrity and availability of information entrusted to us and used in our business. Information security must support reliable products and services, customer trust and our legal and contractual obligations.

This policy applies to all Visar operations, information in all forms, the systems and assets that handle it, and everyone working for or on behalf of Visar. It covers business administration, software development, delivery, support, internal systems and supplier relationships. Customer-specific responsibilities and service commitments are set out in the applicable Terms of Service and customer agreements.

Visar bases its information security management system on ISO/IEC 27001. We aim to strengthen our system security and assurance practices through progressive alignment with relevant requirements in the Swedish Armed Forces' instructions for security accreditation (ISA) and security requirements for information systems (ISK).

This ambition applies across all Visar operations, including business administration, internal systems, development, delivery, support and supplier relationships. It encompasses secure development and delivery, supply-chain assurance, documented security architecture, verification and lifecycle security management. Applicable requirements will be determined according to each system's intended use, protection needs and customer requirements, with detailed assessments and improvement plans documented internally.

This policy provides direction for the information security management system (ISMS). Detailed controls, responsibilities and evidence are maintained in supporting internal documents.

Management commitment and accountability

Management will provide direction and resources, assign responsibilities, promote security awareness and review security performance. Information security requirements must be considered in business decisions and changes.

Information and system owners must identify the assets and risks within their responsibility, determine protection needs and ensure that controls are maintained. Everyone with access must follow applicable requirements and promptly report suspected incidents or weaknesses.

The CTO, coordinates day-to-day information security, assesses risks and recommends safeguards. The CEO owns this policy and decides whether residual risks are acceptable. Significant residual risks must be escalated to the Board of Directors for a decision.

Information and system ownership must be assigned and documented internally.

Security objectives and risk management

Our objectives are to prevent unauthorised access or disclosure, protect information and software from unauthorised change, maintain availability appropriate to business needs, and detect and respond to incidents effectively. We will meet applicable security requirements and continually improve the ISMS.

Security decisions must be based on documented risk assessments that consider likelihood, consequences, legal and contractual requirements, and the needs of customers and other relevant parties. Risk assessments must take place at planned intervals and when significant changes are proposed or occur, in accordance with ISO/IEC 27001. The intervals must be defined in internal ISMS planning, and assessment results must be documented.

Risk treatment must have an accountable owner, selected controls, a target completion date and a recorded decision on residual risk. Exceptions must be documented, time-limited, approved by the designated authority and reviewed. An internal exception cannot waive a legal or contractual obligation.

Detailed security objectives, performance measures, responsibilities, reporting and review arrangements, and risk acceptance criteria must be documented in the internal security plan.

Information classification and handling

Visar's Information classification handbook applies across all Visar operations. Use it to assess confidentiality, integrity and availability independently and select proportionate protection. Preserve applicable customer and third-party markings and handling requirements.

Information owners must define appropriate access, storage, transfer, retention and disposal requirements. Credentials, encryption keys and other information that enables access must receive protection consistent with the information they protect. Publishing information requires authorisation.

Sensitive information must be encrypted in transit and at rest. Technical requirements and key-management procedures must be documented internally.

Identity, access and secure working

Grant access only for authorised duties and the minimum privileges required. Use individual identities where practicable, strong authentication appropriate to risk and enhanced protection for privileged access. Multi-factor authentication is mandatory for remote access and

administrator accounts. Access must be reviewed and removed or changed promptly when duties or engagements change.

Use approved systems, protect devices and credentials, and prevent unauthorised physical and remote access. Sharing information or using an external service requires an assessment of the information's classification and the applicable obligations.

Secure development and operation

Security requirements must be considered throughout software design, development, testing, release and maintenance. Code changes must be reviewed by a person other than their author before release. Control access to source and build systems, protect release integrity and manage third-party dependencies and licence obligations.

Maintain an inventory of relevant assets and dependencies. Assess vulnerabilities and prioritise remediation according to risk and agreed obligations. Use secure configurations, proportionate separation of environments, controlled changes and suitable monitoring.

Record and protect the security events needed for detection, investigation and accountability. Logging must be proportionate, access-controlled and subject to defined retention requirements.

Customer information, privacy and AI

Process personal data lawfully and only for defined purposes, with appropriate minimisation, retention and safeguards. The Privacy Policy describes our processing for individuals; customer agreements and the applicable DPA govern processing on a customer's behalf.

Customer access and support activities require authorisation and must remain within the agreed scope. Protect confidential customer information and do not use it for unrelated purposes.

AI use must follow approved information-handling requirements and the applicable AI policy. We do not use personal data to train or fine-tune models or authorise third parties to do so.

Suppliers and external dependencies

Assess suppliers before granting access to information or relying on their services, and reassess material changes. Suppliers must be bound by written confidentiality and security obligations before receiving access to sensitive information. Agreements must address security responsibilities, confidentiality, personal data, incident notification, relevant subcontractors, and return or deletion of information as appropriate to risk.

Assess processing locations, access arrangements and continuity dependencies. Monitor relevant supplier obligations and ensure that ending a service includes revoking access and handling retained information appropriately.

Incident management and continuity

Report suspected security incidents and weaknesses promptly. Assigned responders must assess and contain incidents, preserve appropriate evidence, coordinate recovery and meet applicable notification duties. Reviews must identify causes and corrective actions.

Report security incidents and vulnerabilities to security@visar-systems.com. The CTO is responsible for coordinating the handling of reports. Reports must be encrypted using the public encryption key for this mailbox.

The public encryption key for security@visar-systems.com is available on the Visar Systems Wiki.

Identify critical activities, dependencies and recovery needs. Maintain protected backups and proportionate continuity and recovery arrangements, supported by appropriate testing. Detailed procedures and testing arrangements must be maintained internally. Recovery priorities and acceptable disruption must be agreed by the responsible owners.

Assurance, awareness and continual improvement

Employees and contractors must receive information security training appropriate to their roles, including onboarding and refresher training. Supporting policies and procedures must be available to those who need them.

Management will monitor agreed objectives, risk treatments, incidents, supplier issues and corrective actions. Internal audits and management reviews of the ISMS must take place at planned intervals in accordance with ISO/IEC 27001. Their schedules, responsibilities, results and resulting actions must be documented internally, with follow-up of nonconformities and opportunities for improvement.

Review this policy at planned intervals and when significant changes occur, including relevant business, legal, contractual or threat changes. The review schedule must be documented internally. Approval, version history and communication of changes must be recorded.

Related documents

Information classification handbook; Privacy Policy; AI Usage Policy; internal security plan; applicable customer agreements and DPA; and supporting risk, access, development, incident and continuity procedures.

ISO/IEC 27001:2022 provides the reference framework for developing the ISMS. Future certification is on the roadmap for 2027.